Cryptology ePrint Archive: Report 2011/435

The IPS Compiler: Optimizations, Variants and Concrete Efficiency

Yehuda Lindell and Benny Pinkas and Eli Oxman

Abstract: In recent work, Ishai, Prabhakaran and Sahai (CRYPTO 2008) presented a new compiler (hereafter the IPS compiler) for constructing protocols that are secure in the presence of malicious adversaries without an honest majority from protocols that are only secure in the presence of semi-honest adversaries. The IPS compiler has many important properties: it provides a radically different way of obtaining security in the presence of malicious adversaries with no honest majority, it is black-box in the underlying semi-honest protocol, and it has excellent asymptotic efficiency.

In this paper, we study the IPS compiler from a number different angles. We present an efficiency improvement of the ``watchlist setup phase" of the compiler that also facilitates a simpler and tighter analysis of the cheating probability. In addition, we present a conceptually simpler variant that uses protocols that are secure in the presence of covert adversaries as its basic building block. This variant can be used to achieve more efficient asymptotic security, as we show regarding black-box constructions of malicious oblivious transfer from semi-honest oblivious transfer. In addition, it deepens our understanding of the model of security in the presence of covert adversaries. Finally, we analyze the IPS compiler from a \emph{concrete efficiency} perspective and demonstrate that in some cases it can be competitive with the best efficient protocols currently known.

Category / Keywords: cryptographic protocols /

Publication Info: An extended abstract appeared at CRYPTO 2011. This is the full version.

Date: received 12 Aug 2011

Contact author: lindell at biu ac il